IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	NO. 1:14 CR-119
	)	
V.	)	Chief Judge Christopher C. Conner
	)	
ROBERT J. RICE,	)	
Defendant	)	

DEFENDANT'S BRIEF IN SUPPORT OF PRETRIAL MOTION TO SUPPRESS EVIDENCE DERIVED FROM DEFICIENT WARRANTS

A. PROCEDURAL HISTORY:

The Defendant was initially charged in Cumberland County, Pennsylvania on April 3, 2013 with 131 counts, alleging violations of Pennsylvania's Crimes Code related to the possession of child pornography. The Commonwealth *nolle processed* its case against the Defendant following the filing of an Indictment in the United States District Court for the Middle District of Pennsylvania on May 14, 2014. *See* Doc. No. 1. The Defendant was charged with two counts of violating the Federal Crimes Code at Title 18, Sections 2252A(a)(5) and (2). *See* Doc. No.1. Trial was initially scheduled for August 12, 2014. *See* Doc. No. 14. However, a number of continuances were filed by both the Defendant and the United States since that date. *See* Doc. Nos. 16-29. Discovery has been ongoing in this matter. The Court has set a motions deadline for October 26, 2015 and trial is presently schedule for December 7, 2015. *See* Doc. No. 29.

B. BRIEF STATEMENT OF THE FACTS

The Defendant and his wife, Marilyn Rice, had a tumultuous marriage in which Mrs. Rice believed her husband was being unfaithful. For over nine years,

Mrs. Rice, without her husband's knowledge or permission, installed various spyware and keylogger programs on the Defendant's personal computer, which she then used to access accounts that were protected by passwords. In particular to this case, Mrs. Rice used a password obtained through one of the keylogger programs to access part of the Defendant's computer which was only accessible to the Defendant in order to install a spyware program called Spector Pro. That program is capable of performing, and in fact did perform, a variety of spyware functions. It can capture every keystroke made on the computer where it is installed, intercept emails and other messages, and it can keep track of all websites visited and capture screen shots. It can be directed to compile a report of this information and forward it to a third party at certain intervals and automatically intercept incoming emails and forward copies to a third party email address. Spector Pro is designed to work in stealth mode and the program goes undetected on a computer, even with an active antivirus program. In this case, Mrs. Rice installed the program on the Defendant's computer on January 23, 2013 and had all information sent to a hidden, password-protected file known and accessible only to Mrs. Rice.

On January 29, 2013, the Defendant moved out of the marital home and discovered that his personal computer was missing. When the Defendant confronted Mrs. Rice, she indicated that she had taken the computer, hidden it and that he would never see the computer again. Between January 29, 2013 and February 7, 2013, Mrs. Rice repeatedly accessed the computer, manipulating, copying, deleting and modifying over 3700 files. On February 7, 2013, Mrs. Rice took the Defendant's computer to the Silver Spring Township Police Department where she informed police that she had placed a spyware program on the Defendant's computer and believed there to be child pornography on his computer. Mrs. Rice reported that she saw pictures of nude children on the computer. Mrs. Rice was then interviewed by Detective Keefer with the Cumberland County Sheriff's Department. This interview

was recorded. During the interview, Mrs. Rice told the detective that the spyware program captured screenshots, websites visited, keystrokes and passwords, and that the program intercepted emails and chats. Mrs. Rice then disclosed the information Spector Pro had intercepted and files she manipulated to the county detectives.

Using only the information obtained by Mrs. Rice through the Spector Pro spyware program, Detective Freeling applied for and obtained a search warrant for the Defendant's computer. Following the search of the computer, police then applied for additional search warrants for the Defendant's hotel room, vehicle, house, office and office computers.

C. QUESTIONS PRESENTED:

i. *Whether the Defendant has a reasonable expectation of privacy in his computer?*

ii. *Whether the warrants based on illegally obtained information must be quashed?*

iii. *Whether the warrants should be quashed and evidence derived therefrom suppressed for a lack of probable cause?*

D. ARGUMENT:

The Constitution affords protection from the government engaging in unreasonable searches or seizures of those places where one has a reasonable expectation of privacy, unless a proper warrant is obtained. Here evidence was unconstitutionally seized from the Defendant's computer when illegally obtained information was used to support probable cause determinations in applications for

search warrants. Because the Defendant had a reasonable expectation of privacy in his computer, and the computer was illegally searched, all evidence derived therefrom should be suppressed.

i. The Defendant has a Reasonable Expectation of Privacy in his Computer

The Fourth Amendment of the U.S. Constitution provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

U.S. Const. Amend. 4. The touchstone of the Fourth Amendment analysis has been whether the person has a constitutionally protected reasonable expectation of privacy. *Oliver v. U.S.*, 466 U.S. 170, 171 (1984), *citing Katz v. United States*, 389 U.S. 347, 360 (1967). The Amendment does not protect merely subjective interests in privacy, but only those expectations which society is prepared to recognize as reasonable. *Id.* A reasonable expectation of privacy is an expectation that has some source outside the Fourth Amendment, "either by reference to concepts of real or personal property law, or to understandings that are recognized and permitted by society." *U.S. v. Jones,* 132 S.Ct. 945, 951 (2012), *citing Minnesota v. Carter*, 525 U.S. 83 (1998).

The Defendant in this case had a reasonable expectation of privacy in his personal computer. The Defendant manifested a subjective expectation of privacy

in his computer in that it was password protected and he did not volunteer this information to other parties. In fact, his computer was only accessed by Mrs. Rice after she obtained his password through a covert spyware program. The contents of his computer were then exposed after his wife illegally installed the Spector Pro spyware program. Defendant's expectation of privacy is one that society is willing to accept as reasonable for two reasons. First, because modern electronic realities require individuals to use personal computers to participate in the modern world, it follows that society is willing to impose an expectation of privacy considering the private and valuable information one stores on their home computer such as financial records, attorney-client correspondence, passwords, and other personal records. Secondly, by virtue of the Wiretap Act, (Title 18, Section 2510 et. seq. of the United States Code), which protects the privacy of communication, society has expressed an expectation of privacy in electronic communication. Because the Defendant expressed a subjective expectation of privacy in his personal computer, and this is a privacy expectation society is willing to accept as reasonable, the Defendant's personal computer was protected against unreasonable searches and seizures under the Fourth Amendment of the United States Constitution.

ii. The Use of Illegally Obtained information in the Affidavit of Probable Cause Violates the Defendant's Fourth Amendment Rights

The search warrants must be quashed because they are based entirely on information illegally intercepted by Mrs. Rice and illegally disclosed and used by the government, in violation of the Federal Wiretap Act, Title 18, Section 2510 et. seq.

The paramount goal of the Wiretap Act was to protect the privacy of individuals in the face of technological advances that made intrusions more prevalent. *United States v. Eady*, 2015 U.S. Dist.N.J., LEXIS 49924 (2015) (internal citations omitted). It was also important to Congress to protect the integrity of the courts by ensuring that they would not become partners to the illegal conduct. *Gelbard v. United States,* 408 U.S. 41 at 51, *quoting* Congressional findings. The Wiretap Act prohibits not just the unlawful interception of private communications, but also the *disclosure* or *use* of unlawfully intercepted communications. Section 2511(1)(c) plainly states that it is unlawful to intentionally disclose or endeavor to disclose, "to any person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection." 18U.S.C.A. 2511(1)(c). Likewise, it shall be unlawful to use the contents of any "wire, oral or electronic communication, knowing or having reason to know that the information was

obtained through the interception of a wire, oral or electronic communication in violation of this subsection." *Id.* At 2511(1)(d). Section 2517(1) and 2517(2) provide an exception for the disclosure and use of intercepted communication by law enforcement officers, but within strict limitations. Any law enforcement officer who *"by any means authorized by this chapter*, has obtained knowledge of the contents of any wire, oral or *electronic communication,* or evidence derived therefrom..." may disclose and/or use such contents to the extent such disclosure and/or use is appropriate to the proper performance of his official duties. 18 U.S.C.S. 2517(1) - (2) (emphasis added).

Relating to probable cause, Section 2517(2) authorizes the way in which law enforcement officers may use intercepted communications in affidavits for warrants. In the legislative history to Title III, Congress states that section 2517(2) "envisions use of the contents of intercepted communications, for example, to establish probable cause for arrest, to establish probable cause to search, or to develop witnesses." S.Rep. No. 1097, *supra,* at 2188 (internal citations omitted). But in authorizing law enforcement officers to use intercepted communication to establish probable cause, Congress places a strict caveat that the officer must have learned of the information *"by any means authorized by this chapter."* This prescription reflects Congressional concerns that government agents might become partners to the illegal activity that the Wiretap Act sough to prohibit.

In the present case, the interception of the electronic communication on the Defendant's computer by Mrs. Rice constituted an illegal wiretap, as more fully explained in Defendant's Brief in Support of Pretrial Motion to Suppress Evidence Obtained in Violation of Federal Wiretap Act, filed contemporaneously with all of Defendant's pre-trial motions and supporting briefs. When Mrs. Rice disclosed this information to the police, the Wiretap Act was again violated under Section 2511(1)(c). When the illegally obtained information was used by police and disclosed in their first affidavit of probable cause to obtain a search warrant, that use and disclosure was not authorized under Section 2517(1) and (2) but were further violations of Sections 2511(1)(c) and (d). Each time the police applied for additional search warrants, they violated the Wiretap Act when they disclosed and used the illegally obtained information which they did not learn of *"by any means authorized by this chapter"* to support probable cause.

The remedy for the government's repeated violations of the 18 U.S.C.A Section 2511(1)(c) and (d), 2517(1) and 2517(2) is clear. The illegally used information must be excised from the affidavit for search warrant and the warrant must be reevaluated for probable cause. As it relates to the initial search warrant for the Defendant's computer, if the illegally disclosed and used information is excised, nothing remains to establish probable cause and the search warrant along

with all evidence derived therefrom, including subsequent warrants, must be suppressed.

The government may argue that under Section 2515 there is no provision in the Wiretap Act for suppression of electronic communications. This argument must fail for several reasons. First, Section 2515 mandates exclusion of illegally intercepted wire and oral communication offered as evidence at trial or other proceedings. Section 2515 clearly relates to the testimonial disclosure of intercepted communications regulated by Section 2517(3) and not to the appropriate use of intercepted communications to establish probable cause regulated by Section 2517(2). Second, to allow the government to illegally use information it illegally obtained to support probable cause would eviscerate Section 2517(2). Third, to condone the government's illegal use of information it illegally obtained to establish probable cause would encourage government agents to become participants in the illegal conduct that the Wiretap Act seeks to prevent. Finally, the use of illegally obtained information as its sole basis for probable cause in a search warrant violates the Defendant's Fourth Amendment protection against unreasonable searches and seizures.

For these reasons, all information illegally obtained by the police from Mrs. Rice and illegally used by the police to establish probable cause to search the

Defendant's computer must be excised from the affidavit and the search warrant must be reevaluated for probable cause.

iii. Affidavits of Probable Cause Fail to Contain Sufficient Facts to Establish Probable Cause

In the alternative, if it is found that the affidavit did not contain illegally obtained information, the warrant must still be quashed because it fails to establish probable cause.

> "Probable cause is a 'fluid concept that 'turn[s] on the assessment of probabilities in particular factual contexts.'" *U.S. v. Stearn*, 597 F.3d at 554 (*quoting Gates*, 462 U.S. at 232). In deciding whether probable cause exists, the court must weigh "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Id.* (*quoting Gates*, 462 U.S. at 231). "Statements in an affidavit may not be read in isolation—the affidavit must be read as a whole." *U.S. v. Whitner,* 219 F.3d at 296 (*quoting Conley*, 4 F.3d at 1208).

United States v. Rafferty, 2014 U.S. Dist. LEXIS 92214, *17, 2014 WL 3109961 (E.D. Pa. July 8, 2014). The police here intended to look for evidence of child pornography when they applied for their search warrant for the Defendant's computer. Child pornography is defined as "any visual depiction... of sexually explicit conduct, where- ...the depiction involves the use of a minor engaging in sexually explicit conduct..." 18 U.S.C.A. § 2256(8). Sexually explicit conduct is defined as "acted or simulated sexual intercourse, bestiality, masturbation or sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area

of any person." 18 U.S.C.A. § 2256(2)(a). The Third Circuit has adopted the six-factor Dost test for determining whether an image includes a "lascivious exhibition of the genitals":

> 1) whether the focal point of the image is on the child's genitalia . . . ; 2) whether the setting is sexually suggestive, i.e., in a place or pose generally associated with sexual activity; 3) whether the child is depicted in an unnatural pose . . . considering the age of the child; 4) whether the child is fully or partially clothed, or nude; 5) whether the image suggests sexual coyness or a willingness to engaged in sexual activity; 6) whether the image is intended or designed to elicit a sexual response in the viewer.

United States v. Rafferty, 2014 U.S. Dist. LEXIS 92214, *17, 2014 WL 3109961 (E.D. Pa. July 8, 2014), *quoting United States v. Villard*, 885 F.2d 117, 122 (3d Cir. 1989) (*quoting United States v. Dost,* 636 F. Supp. 828, 831 (S.D. Cal. 1986)). A qualifying image will satisfy more than one factor, but need not satisfy all. Id.

In this case, the affidavit of probable cause contained the following descriptions: "pictures of three (3) or four (4) females performing oral sex"; "photographs depicting child pornography"; "a picture of a four (4) year old female with her legs spread and a penis between the aforementioned child's legs."; and "chat room/internet conversations between her (Marilyn Rice) husband and other individuals relating to the exchange of pornographic photographs of children." There are no other descriptions of the child pornography contained in the affidavit, nor did the magistrate view any content prior to the issuance of the

first search warrant. The affidavit contains no claim of any nudity involving minors, nor any claim that minors were engaged in explicit sexual activity as defined by 18 U.S.C.A. § 2256(2), nor any claim of lascivious display of genitals. The descriptions in the affidavit do not satisfy any of the *Dost* factors and are merely conclusory in nature. Therefore, the warrant is lacking in probable cause and must be quashed.

Conclusion

WHEREFORE, The Defendant respectfully requests that the warrants be quashed and any evidence obtained based on these search warrants suppressed.

Respectfully Submitted,

Date: 10/26/15

/s/ Joseph D. Caraciolo

Joseph D. Caraciolo, Esquire
Attorney ID No. 90919
112 Market Street, 6th Floor
Harrisburg, PA 17101
Telephone (717) 236-9391
Facsimile (717) 236-6602